David Grout, McAfee : « sur la sécurité, les entreprises sont ambivalentes »

Une récente étude de McAfee, baptisée *Network Performance and Security*, mettait en évidence que plus de la moitié (54 %) des entreprises désactivent certaines fonctions de leurs firewall (l'analyse des paquets en tête) pour privilégier les performances du réseau. Un chiffre étonnant autant qu'inquiétant. *« Le phénomène n'est pas nouveau*, assure David Grout, directeur Europe du Sud de McAfee, ***l'équilibre entre protection de l'entreprise et contraintes business perdure depuis 10 ans****. »*

Pourtant, les problématiques de sécurité sont loin d'être négligées. A titre d'exemple, une autre étude, réalisée par Evalueserve toujours pour McAfee, indiquait mi-novembre dernier que 71% des DSI en France considèrent les attaques ciblées comme une préoccupation majeure. *« Il y a une ambivalence complète entre la désactivation des fonctions de sécurité et les problématiques qu'elles peuvent causer*, poursuit le responsable. ***La sécurité est souvent la première priorité des entreprises qui peuvent changer d'avis 5 minutes plus tard*** *car elles exigent aussi un réseau 100% disponible sans aucune latence, ni ralentissement. »*

Incorporer la sécurité au plus bas niveau

Or, la sécurité a toujours un impact sur les performances, même si les technologies en ce domaine ont suivi un équivalent à la loi de Moore en offrant toujours plus de fonctionnalités de protection à ressources de calcul et coûts stables au fil des ans. *« Notre travail est de* ***réduire au maximum les contraintes*** », rappelle David Grout. Ce qui passe aujourd'hui par l'intégration de la sécurité en amont de la conception des produits (security by design) mais aussi par le *fine tuning*. Autrement dit, *« incorporer au plus bas niveau, processeur ou logiciel, les éléments de sécurité »*.

David Grout assure qu'Intel, propriétaire de McAfee, n'intègre pas de fonctions spécifiques de l'éditeur de sécurité dans ses processeurs pour optimiser les performances de ses produits. *« Au contraire, Intel conserve un esprit d'ouverture, notamment en proposant ses API V-Pro à l'ensemble du marché »*, affirme notre interlocuteur en évoquant les technologies de prise de contrôle à distance des PC intégrées aux chipsets d'Intel. Si le fondeur de Santa Clara n'entend pas favoriser au niveau hardware les développements de sa filiale, McAfee travaille en revanche sur deux axes pour tirer parti des technologies silicium de sa maison mère. Le premier vise à **améliorer les performances de traitements à travers l'appel des instructions**. *« Depuis 3 ans environ, nous précisons à Intel ce dont nous avons besoin pour améliorer les performances de sécurité avec des instructions taillées en conséquence pour protéger des éléments. »* Le second axe entend **tirer parti des éléments de sécurité intégrés aux Core et autres Xeon** comme le chiffrement AES-NI par exemple. Autant d'interactions qui transparaitront à travers les produits qu'Intel présentera au deuxième semestre 2015. Peut-être dès les futurs cœurs Skylake ? David Grout n'était pas en mesure de le confirmer.

Mais la protection de l'entreprise passe aussi par **une nouvelle approche de la sécurité**, non plus en silo mais plus globale. *« Il faut orchestrer et faire profiter les technologies les unes des autres »*, estime David Grout. Une approche de « sécurité connectée » (*connected security*) qui se traduit chez

McAfee par Threat Intelligence Exchange (TIE). Cette solution de prévention des menaces s'appuie notamment sur Data Exchange Layer (DXL), un protocole de communication bidirectionnel temps réel en liaison avec les différents éléments du réseau (passerelles, end-point, autres produits de sécurité) afin de partager les informations et les faire travailler de manière unifiée. Une unification que McAfee concrétise à travers son offre NetGen Firewall et la technologie Stonesoft (racheté en 2013) de détection des intrusions granulaires, présentée dans une console unifiée avec des fonctions d'agrégation de lignes ADSL (pour remplacer les liaisons MPLS) et de clustering (pour assurer la disponibilité du réseau).

Orchestrer et automatiser

Pour David Grout, la tendance est aujourd'hui clairement à l'orchestration et l'automatisation des fonctions de sécurité. *« Si on ne s'y tourne pas,* ***on passe son temps à coller des rustines et à courir après les alertes de sécurité****. »* Si l'orchestration est un concept vieux de plus de 10 ans et bien intégré, *« l'idée est aujourd'hui de dépasser le end-point pour se porter sur la donnée et partager les informations sur les caractéristiques des codes malveillants avec les concurrents »*. Ce dont se charge DXL commercialisé depuis octobre dernier, suite à sa présentation lors de l'événement Focus de l'éditeur. *« Rester seul dans son coin ne suffit plus, on ne peut pas tout couvrir seul, il faut partager la connaissance. »* En septembre dernier, McAfee a ainsi rejoint Palo Alto Networks, Fortinet et Symantec dans la première *cyber threat alliance* visant à coordonner les efforts de l'industrie pour lutter contre les menaces numériques. McAfee déclare également travailler avec Europol et l'Otan dans cet esprit.

Quand à l'automatisation, concept plus récent, elle vise à automatiser des tâches selon une politique de sécurité (par exemple mettre en quarantaine une machine qui émet plus de 40 alertes par jour) pour limiter les risques de propagation et **laisser le temps aux équipes techniques d'investiguer en profondeur**. *« Seulement 5 ou 10 % de machines automatisées soulage les équipes »*, indique David Grout qui n'envisage pas une automatisation complète de l'infrastructure, tout au mieux 30 ou 40% dans quelques années. *« Cela dépend des entreprises qui peuvent automatiser entre quelques pour cent des équipements et jusqu'à 20 %. Mais 3 ou 4 %, c'est déjà une belle étape franchie pour une entreprise aujourd'hui. »*

Lire également
Laurent MARECHAL, McAfee : « la sécurité n'est plus une option »